

Content Server

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration

Global Information Services

2. System Information

- (a) Name of system: Content Server
- (b) Bureau: Office of the Legal Adviser (L)
- (c) System acronym: CS
- (d) iMatrix Asset ID Number: 227232
- (e) Reason for performing PIA: Click here to enter text.
 - ☒ New system
 - ☐ Significant modification to an existing system
 - ☐ To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
 - ☒ Yes
 - ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?

The Assessment and Authorization process is underway and CS is expected to receive an Authorization-To-Operate by October 2017.
- (c) Describe the purpose of the system:

Content Server is a commercial off-the-shelf/ government off-the-shelf (COTS/GOTS) product that is used in L for electronic records and content management in order to store various types of legal and administrative information and data. Access to Content Server is only granted to employees of L.
- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The system contains legal opinions and briefs, client information, and HR information. This data includes first name, last name, date and place of birth, contact information, SSN, home address.

- (e) What are the specific legal authorities and/or agreements that allow the information to be collected?

5 U.S.C. 301, 42 U.S.C. 659, 42 U.S.C. 666, 5 CFR part 581, Public Law 71-715

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒ Yes, provide:

- SORN Name and Number: Legal Case Management Records, STATE-21
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 22, 2016

☐ No, explain how the information is retrieved without a personal identifier.

[Click here to enter text.](#)

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐ Yes ☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☐ Yes ☒ No We are currently working on the records retention schedule.

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): [Click here to enter text.](#)
- Length of time the information is retained in the system: [Click here to enter text.](#)
- Type of information retained in the system:
[Click here to enter text.](#)

4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

☐ Members of the Public

☒ U.S. Government employees/Contractor employees

☐ Other (people who are not U.S. Citizens or LPRs)

- (b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒ Yes ☐ No

- If yes, under what authorization? 5 U.S.C. 301, 42 U.S.C. 659, 42 U.S.C. 666, 5 CFR part 581, Public Law 71-715

,

- (c) How is the information collected?

Content Server users directly type the information into a document that is saved into Content Server. However, the information is normally from another source, e.g Global Employee Management System (GEMS), the TORTS system, Holocaust Claims Deportation Tracking System (HCDTS), interview notes, recruitment notes, email, etc. Content Server does not connect to any other systems. Note that TORTS is not an acronym for a system. A Tort is when someone from the outside sues the Dept., and the database we use to track them is called TORTS.

(d) Where is the information housed?

- ☒ Department-owned equipment
- ☐ FEDRAMP-certified cloud
- ☐ Other Federal agency equipment or cloud
- ☐ Other

- If you did not select "Department-owned equipment," please specify.

[Click here to enter text.](#)

(e) What process is used to determine if the information is accurate?

None, as the information that is entered into Content Server is coming from another source such as email, recruitment notes, interview notes, etc. The originating source has the responsibility to maintain accurate information.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Content Server does not collect information directly from the source. Ensuring the information is current is the responsibility of the office that originally collected the information.

(g) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial sources or publicly available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

Content Server does not collect information directly from the source. Notice is provided by the owning office at the initial point of collection

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐ Yes ☒ No

- If yes, how do individuals grant consent?

[Click here to enter text.](#)

- If no, why are individuals not allowed to provide consent?

Content Server does not collect information directly from the source. Individuals grant consent at the initial point of collection by the owning source (e.g., GEMS, TORTS, HCDTS, interview notes, recruitment notes, email, etc.).

(j) How did privacy concerns influence the determination of what information would be collected by the system?

Only the minimum amount of information absolutely necessary is stored in Content Server.

5. Use of information

- (a) What is/are the intended use(s) for the information?

The information stored in Content Server is used for reference in compiling information for the L-H/EX HR team, for the L Recruitment Committee, and L-H/EX management as well as for case analysis.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes

- (c) Does the system analyze the information stored in it? ☐ Yes ☒ No

If yes:

- (1) What types of methods are used to analyze the information?

[Click here to enter text.](#)

- (2) Does the analysis result in new information?

[Click here to enter text.](#)

- (3) Will the new information be placed in the individual's record? ☐ Yes ☐ No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

☐ Yes ☐ No

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The information in Content Server is shared internally with attorneys and other authorized personnel in L. No information is shared outside of L.

- (b) What information will be shared?

Any information that is stored in Content Server, *and* that the particular user has access to, can be shared within L. Users only have permissions to the office folders that correspond to their office.

- (c) What is the purpose for sharing the information?

Information is shared for legal collaboration such as comparing case notes and discussions of hiring decisions with members of the L Recruitment Committee. The Recruitment Committee is a group within L that makes hiring recommendations for the attorneys and other staff to the L Front Office.

- (d) The information to be shared is transmitted or disclosed by what methods?

Information is shared via email and hand carried paper printout.

- (e) What safeguards are in place for each internal or external sharing arrangement?

All employees have taken the appropriate PII and cyber security courses and understand the importance of maintaining the confidentiality of data.

- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Sharing information could result in unauthorized exposure of PII. This concern is mitigated by only sharing with individuals who have a need to know the information and including the minimum amount of information in any transmission. While there is no risk of damage to the U.S. government, there is a risk of personal embarrassment and economic loss if certain information were to be shared inappropriately. This is another reason why the document repository is restricted to each L office. In other words, an attorney in the Political Military office (L/PM) would not have access to the Employment Law (L/EMP) folder, because the individual does not have a need to know.

7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?

Content Server does not collect directly from the source. Individuals wishing to gain access to their information must follow the procedures set forth by the originating system.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐ Yes ☒ No

If yes, explain the procedures.

[Click here to enter text.](#)

If no, explain why not.

The information does not originate in Content Server. Any amendments must be made with the owning system.

- (c) By what means are individuals notified of the procedures to correct their information?

Individuals are notified of the procedures to correct their information by the originating system.

8. Security Controls

- (a) How is the information in the system secured?

Content Server stores its metadata in a back end database, and the content itself is stored as encrypted files on a file server.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

The folder structure in Content Server is organized by office folder. Only the members of that office have permissions to that office’s folders. Also within the office folder structure, there are certain folders only the Assistant Legal Adviser (equivalent to an Office Director) have access to. This is also true of the Executive Office – only members of the HR division have access to the HR folders within the main EX folder.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Content Server maintains an extensive audit trail that details who accesses what file, when that file was accessed, and what was done to the file.

- (d) Explain the privacy training provided to authorized users of the system.

All users are required to complete the PS800 Cyber Security Awareness training within 10 days of receiving their network account, and are also required to take PA459, Protecting Personally Identifiable Information course.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒ Yes ☐ No
If yes, please explain.

Only authorized users have access to their office's folders and files in Content Server.

- (f) How were the security measures above influenced by the type of information collected?

When the system was set up, it was decided that not all employees needed access to all of the content in the system. Content Server allows different levels of security on every object within it. For example, for sensitive HR documents, folder level security is placed on those documents so that only members of the HR team can see them. No one else in the bureau can see them.

9. Data Access

- (a) Who has access to data in the system?

End users have only the level of access necessary by their office.

- (b) How is access to data in the system determined?

Each user's office director must request the creation of a new account. The Content Server administrators create the Content Server accounts and put them into the appropriate group based on the individual's office. Each end user only has access to their office folder.

- (c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☐ Yes ☒ No

- (d) Will all users have access to all data in the system, or will user access be restricted?
Please explain.

User access is restricted to individual offices, i.e., users only have access to their office folder.

- (e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Every action in Content Server is audited. Every time a document is opened, browsed, or edited, the action is written to a database table in Content Server.